APPENDIX A

Digital River Fraud Prevention Technology

Fraud has become one of the largest obstacles many companies encounter when trying to conduct electronic commerce from their Web sites. Several firms have begun selling via the Internet only to learn that thieves, who have cracked their system using a stolen or fabricated credit card, account for a large percentage of their orders. Though the media has publicized the need for greater protection for consumers online, it is the online merchants that have recently recognized that the greater risk is their own.

Recent national media attention has focused specifically on the prevention of fraud in connection with software sales transactions completed over the Internet. A recent *New York Times* article quotes the chief executive officer of an online software retailer, whose company was experiencing more fraud than actual sales, virtually driving the firm out of business.

There are four primary issues surrounding fraud and electronic software distribution:

- Fraud Identification and Prevention
- Protection of Intellectual Properties
- Prevention of Credit Card Number Theft
- Control Through Auditing Processes

Digital River's fraud system functions effectively on all of these fronts. This system allows Digital River to store files securely, and deliver digital information via secure connections and audited processes, while protecting against financial losses due to fraud.

Fraud Identification and Prevention:

Several firms engaged in Internet software commerce have reported credit card fraud figures typically approaching 20% per day, with some software sellers recording losses in the 50% range on specific days. Internet fraud losses at these levels are substantially higher than with traditional mail and telephone orders. Without advanced detection tools, fraud could put the entire concept of selling software via the Internet at significant risk.

Online merchants selling goods for physical distribution may be able to weed out fraudulent orders by manually reviewing each order that is placed. For example, closely scrutinizing each order having a shipping address that is different than that of the credit card holder can be a possible way to identify fraud. However, online merchants selling software can be especially vulnerable to fraudulent orders if they are not properly prepared to screen them out.

Prevention of loss from Internet fraud demands extensive security procedures and processes, which can demand a massive investment on the part of software developers. Digital River employs the measures described below in their business as the largest source of inventory, transactions, and fulfillment of software products on the Internet.

Digital River's fraud identification procedures have allowed the company to drive fraud to a level significantly below that seen elsewhere in the online software delivery industry. Digital River's current fraud rate is approximately 2% of sales, and their goal is to drop that number below 1% in 1998. The key to this success has been Digital River's multi-tiered fraud detection systems.

Digital River utilizes heuristic logic to model potential thieves through automated qualitative and quantitative detection systems. The American Heritage dictionary defines heuristic as, "Of an educational method in which students learn through investigation and discovery." Digital River's intelligent system will learn from past security breaches, and log them into the "learning" model. This qualitative data is then utilized to screen out fraudulent orders when monitoring future order attempts.

This logic works first by monitoring the movement and actions of each user that enters the commerce system. Consumer actions that mimic those used by hackers receive a higher score than customers that act and flow through the site like a typical honest shopper. Digital River has identified hundreds of actions that are typical only of would-be thieves. These are closely monitored by the system, and when it determines the actions are typical of a thief, the sales transaction is disallowed.

Concurrently, a network management system "observes" all the traffic through the server and takes "snapshots," matching them against approved system procedures and eliminating

access through a "back door." Experienced hackers are thus blocked from any unauthorized accesses.

Quantitative analysis is also utilized in the logic processes to identify potential fraudulent orders. Historical order records provide information to the fraud database that can be referenced each time that an order attempt is made. Digital River uses this database as a reference for each order to identify those that exhibit unusual quantitative characteristics. In this way, the system gains valuable information from the order size, dollar volume, number of orders, IP address, "cookie", and historical customer data. This information is compared to the extensive database of known fraud offenders. The system then kicks out any orders that contain information associated with past fraudulent orders, or exhibit characteristics matching those of the archetypal thief.

Digital River is able to prevent most fraudulent orders through these qualitative and quantitative scoring mechanisms, while allowing real customers to make online purchases quickly and easily.

Protection of Intellectual Properties:

Protection of software intellectual properties is of prime interest to software developers. Potential for loss due to unauthorized reproduction and distribution of software can literally involve millions of dollars. Though copyright laws can protect developers against this type of theft, the time and legal expense required to recover damages are substantial. Extensive circulation of unauthorized copies of software can begin to put the software in the position of being in the public domain, endangering the copyright itself.

Protection of the software products themselves is the highest priority for Digital River security. Their digital inventory is protected behind secured firewalls so that it cannot be accessed by unauthorized users. Secure electronic software distribution through Digital River can reduce the unauthorized duplication and distribution of copyrighted materials, since there are no diskettes to copy or trade. Digital River maximizes this security by limiting the number of approved downloads, and only allows them to take place within five days of a customer purchase. Digital River's

secure servers provide the complete security solution needed to protect the sensitive electronic data of their clients.

Prevention of Credit Card Number Theft:

Consumer fear of fraud can also limit Internet sales of software. Though there is no more inherent risk for consumers using their credit cards to make Internet purchases than for other types of purchases, the perception of consumers is that the risk is substantially higher than in other sales mediums. Consumers are willing to provide their credit card numbers and expiration dates to telemarketers, but are hesitant to give the same information for Internet sales. This has the effect of limiting sales of software through the most direct and convenient medium, the Internet.

In reality, credit card transactions via the Internet can be much safer than conventional means when the appropriate security technology is employed. Digital River employs Secure Sockets Layer (SSL) technology to encrypt transmissions from both the server and end-user sites. The transmissions are encrypted using public and private key technologies that assign undetectable codes to data transmissions to and from the server. Each transmission between Digital River's server and consumer are a matched pair, so that only data from these two sources can be valid. By utilizing this technology, Digital River ensures that external parties can view no credit card numbers or other sensitive information.

The company is planning communications to inform consumers that they can be "sure of security" for their credit card numbers when they see the Digital River secure logo. This approach is designed to inform consumers of Digital River's security precautions and encourage their purchase of additional products.

Digital River's fraud prevention system also ensures the privacy of buyers and their relationship with specific software providers. The privacy of each ISV's list of buyers is maintained through passwords and encryption. One software vendor can see who has bought its products, but cannot see the names of persons buying from other vendors.

The security systems employed by Digital River are fluid and flexible. This is necessary to catch and deter the

innovative, changing efforts of thieves and hackers whose tactics are increasingly imaginative. Additionally, Digital River employees round-the-clock monitoring of systems and security techniques to ensure that no creative hacker can enter the system.

Control Through Auditing Processes:

Digital River has developed complete accounting processes to ensure accuracy. Tying out credit card receipts with system records does this. Each day the sales summary is matched to the credit card report. Summary reconciled data is then matched to the daily credit card deposits on the company's bank statement. Digital River's system ensures accuracy through cross-footing records from internal data, such as server logs, with external records like credit card transactions.

For a third-party review, Digital River's financial statements are audited annually by Arthur Andersen LLP. Also, Arthur Andersen uses sampling techniques to compare transactions to Digital River sales receipts.

In summary, Digital River's multi-tiered fraud system works on four key fronts: fraud identification, protection of intellectual properties, prevention of credit card number theft and control through the auditing process. With these systems in place, Digital River is able to store files electronically and securely, deliver the information to consumers via secure connections and audited processes, while protecting against financial losses due to fraud. Since these systems are fully automated and scaleable, Digital River will no doubt have the capacity to handle nearly any electronic commerce situation presented.